



Alaska Land Mobile Radio System Incident Response Policy

1. Applicability

This policy applies to all employees, contractors, consultants, temporary employees, and other personnel assigned to the Alaska Land Mobile Radio (ALMR) Communications System in the event of a system incident. Any revision or update of this policy must be approved by the User Council.

2. Policy

ALMR shall have a Computer Security Incident Response Capability to address required actions for the creation, implementation, and management of an Incident Response Team to address computer security incidents including, but not limited to, theft, misuse of data, intrusions, hostile probes, and malicious software.


3. Procedures

A system incident is defined as any adverse event threatening the confidentiality, integrity, or availability of ALMR information assets, information systems, and supporting networks. Adverse events may include the insertion of malicious code (e.g. viruses, Trojan horses, or backdoors), unauthorized or unapproved scans or probes, successful and unsuccessful intrusions, and insider attacks. Any violation of ALMR formal security policies, or acceptable use policies, is also defined as an incident.

In response to a System incident, the System Management Office, Security Manager/Information Assurance Officer shall determine the severity of the incident, notify the appropriate personnel, activate an Incident Response Team, and perform all required actions in accordance with the ALMR System Incident Response Procedure 400-2.

4. Effective Date

This policy shall become effective upon signature and shall remain in effect until rescinded. The policy shall be reviewed periodically and updated, as required.

 12-29-10

Del Smith
Operations Manager
Alaska Land Mobile Radio